

#2

Attorney Docket No.: 04329.2320

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of

Tooru KAMIBAYASHI et al.

Serial No.: 09/594,011

Filed: June 15, 2000



Group Art Unit: 2754

Examiner: Not Assigned

For: STORAGE MEDIUM AND CONTENTS PROTECTION METHOD USING
THE STORAGE MEDIUM

CLAIM FOR PRIORITY

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

Under the provisions of 35 U.S.C. § 119, Applicants hereby claim the
benefit of the filing date of Japanese Patent Application No. 11-169980, filed on
June 16, 1999, for the above-identified U.S. patent application.

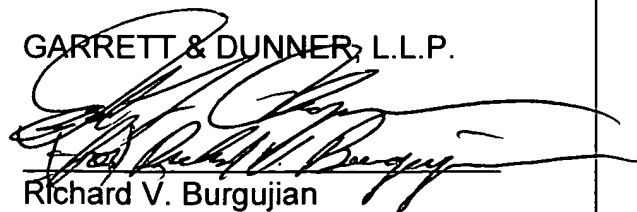
In support of this claim for priority, enclosed is one certified copy of the
priority application.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,

GARRETT & DUNNER, L.L.P.

By:


Richard V. Burgujian
Reg. No. 31,744

ERNEST F. CHAPMAN
Reg. No. 25,961

Date: October 30, 2000
RVB/FPD/sci
Enclosures

LAW OFFICES

FINNEGAN, HENDERSON,
FARABOW, GARRETT,
& DUNNER, L.L.P.
1300 I STREET, N. W.
WASHINGTON, DC 20005
202-408-4000

日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT



別紙添付の書類に記載されている事項は下記の出願書類に記載されて
る事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
in this Office.

出 願 年 月 日
Date of Application:

1999年 6月16日

出 願 番 号
Application Number:

平成11年特許願第169980号

出 願 人
Applicant(s):

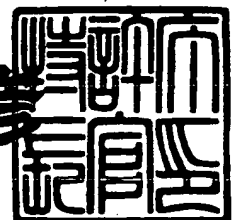
株式会社東芝
松下電器産業株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2000年 6月23日

特許庁長官
Commissioner,
Patent Office

近 藤 隆 彦



出証番号 出証特2000-3046671

【書類名】 特許願

【整理番号】 A009903627

【提出日】 平成11年 6月16日

【あて先】 特許庁長官 殿

【国際特許分類】 G06F 12/00

【発明の名称】 記憶媒体及び同媒体を使用したコンテンツ保護方法

【請求項の数】 6

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝研究開発センター内

 【氏名】 上林 達

【発明者】

 【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝本社事務所内

 【氏名】 山田 尚志

【発明者】

 【住所又は居所】 神奈川県川崎市幸区小向東芝町 1 番地 株式会社東芝マイクロエレクトロニクスセンター内

 【氏名】 岩崎 博

【発明者】

 【住所又は居所】 東京都港区芝浦一丁目 1 番 1 号 株式会社東芝本社事務所内

 【氏名】 田村 正文

【発明者】

 【住所又は居所】 東京都青梅市末広町 2 丁目 9 番地 株式会社東芝青梅工場内

 【氏名】 石橋 泰博

【発明者】

 【住所又は居所】 東京都府中市東芝町 1 番地 株式会社東芝府中工場内

【氏名】 加藤 拓

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 館林 誠

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 原田 俊治

【発明者】

【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内

【氏名】 勝田 昇

【特許出願人】

【識別番号】 000003078

【氏名又は名称】 株式会社 東芝

【特許出願人】

【識別番号】 000005821

【氏名又は名称】 松下電器産業株式会社

【代理人】

【識別番号】 100058479

【弁理士】

【氏名又は名称】 鈴江 武彦

【電話番号】 03-3502-3181

【選任した代理人】

【識別番号】 100084618

【弁理士】

【氏名又は名称】 村松 貞男

【選任した代理人】

【識別番号】 100068814

【弁理士】

【氏名又は名称】 坪井 淳

【選任した代理人】

【識別番号】 100092196

【弁理士】

【氏名又は名称】 橋本 良郎

【選任した代理人】

【識別番号】 100091351

【弁理士】

【氏名又は名称】 河野 哲

【選任した代理人】

【識別番号】 100088683

【弁理士】

【氏名又は名称】 中村 誠

【手数料の表示】

【予納台帳番号】 011567

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9705037

【ブルーフの要否】 要

【書類名】 明細書

【発明の名称】 記憶媒体及び同媒体を使用したコンテンツ保護方法

【特許請求の範囲】

【請求項 1】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体であって、

コンテンツ保護のために無効化すべき電子機器が判別可能なりボケーション情報が予め登録された特定記憶領域を具備し、

前記記憶媒体が任意の電子機器に装着されて使用される場合に、当該電子機器の無効化を前記ボケーション情報に従って制御可能としたことを特徴とする記憶媒体。

【請求項 2】 前記記憶媒体が任意の電子機器に装着されて使用される場合に、当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記ボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するコントローラを更に具備することを特徴とする請求項 1 記載の記憶媒体。

【請求項 3】 前記特定記憶領域が、読み出し専用の不揮発性メモリ上に確保された記憶領域であることを特徴とする請求項 1 記載の記憶媒体。

【請求項 4】 前記特定記憶領域が、書き換え可能な不揮発性メモリ上に確保された、秘匿された特定手続以外ではアクセスできない記憶領域であることを特徴とする請求項 1 記載の記憶媒体。

【請求項 5】 デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶媒体に特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なりボケーション情報を予め登録しておき、前記記憶媒体の 1 つが任意の電子機器に装着されて使用される場合に、前記ボケーション情報に従って当該電子機器の無効化を制御するようにしたことを特徴とするコンテンツ保護方法。

【請求項 6】 デジタルコンテンツの記録機能または再生機能の少なくとも

一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能な記憶メディア部とコントローラとが一体化された記憶媒体のそれぞれに特定記憶領域を設けて、当該特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なりボケーション情報を予め登録しておく、

前記記憶媒体の1つが任意の電子機器に装着されて使用される場合に、その記憶媒体上の前記コントローラにて当該電子機器から当該電子機器を表す情報を受け取って、その情報により前記リボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するようにしたことを特徴とするコンテンツ保護方法。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】

本発明は、画像データや音楽データに代表される種々のデジタルコンテンツを記録再生するのに用いられる記憶媒体に係り、特に不当な電子機器によるコンテンツの記録再生を抑止するのに好適な記憶媒体及び同媒体を使用したコンテンツ保護方法に関する。

【0002】

【従来の技術】

近年、コンピュータ技術の発達に伴い、マルチメディア対応のパーソナルコンピュータ、セットトップボックス、プレーヤー、ゲーム機などの各種電子機器が開発されている。この種の電子機器は、記録メディアに格納された画像データや音楽データなど様々なデジタルコンテンツを再生できるほか、インターネット等を通じてデジタルコンテンツをダウンロードして使用することもできる。

【0003】

これらのデジタルコンテンツは、例えばMPEG2、MP3といったデジタル符号化技術の採用により、品質を落とすことなくコピーしたり、ダウンロードすることができる。このため、最近では、著作権保護の観点から、このようなデジタルコンテンツを不正使用から保護するための技術の必要性が叫ばれている。

【0004】

【発明が解決しようとする課題】

しかし、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器で用いられる記憶媒体は、別の機器に移動しても記録／再生できるリバーシブルなものが多く、その仕様は基本的にはオープンである。このためコンテンツの移動／コピーを自由に行うことができるので、記憶媒体に記憶されたコンテンツを不正なコピー／移動から保護することは實際上困難である。

【0005】

そこで、メモ리카ードのように記憶メディア部とコントローラとが一体化された記憶媒体については、秘匿された特定手続にてのみアクセスでき、ユーザからはアクセスできないアクセス不能領域（秘匿領域）を設け、そこにコピー制御情報、移動制御情報などの、コンテンツの使用に必要な重要な情報を格納しておくことにより、コンテンツの保護を図ることが考えられる。

【0006】

この場合、パーソナルコンピュータ、セットトップボックス、プレーヤーなどの電子機器と記憶媒体の間でコンテンツのコピー／移動を行う際には、それぞれが、著作権保護（コンテンツ保護）に関する所定の仕組み（つまり所定のコンテンツ保護機能）を共有している正当なものであるかを相互に認証し、正しいと認証できた場合に相互に共有する鍵生成のアルゴリズムに従って鍵交換を行って個別に共通の認証鍵を取得し、その認証鍵をコンテンツキー（コンテンツを暗号化するキー）の暗号化（ライセンス暗号化）／復号化またはコンテンツの暗号化／復号化に用いることも考えられる。

【0007】

ところが、上記相互認証に必要な情報は、機器の出荷段階で予め設定されていることから、機器の購入後に当該機器（上で動作するプログラム）が改変されるといった攻撃により、例えばコンテンツ保護の仕組みが無用なものになった場合等においては、上記相互認証だけでは、この種の、問題のある機器を検出できないことになる。

【0008】

本発明は上記事情を考慮してなされたものでその目的は、特定記憶領域に、コ

コンテンツ保護のために無効化すべき電子機器が判別可能なりボケーション情報が予め登録された構成とすることで、当該ボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能な記憶媒体及び同媒体を使用したコンテンツ保護方法を提供することにある。

【0009】

【課題を解決するための手段】

本発明の記憶媒体は、デジタルコンテンツの記録機能または再生機能の少なくとも一方を有する電子機器によるデジタルコンテンツの記録または再生に利用可能であって、コンテンツ保護のために無効化すべき電子機器が判別可能なりボケーション情報が予め登録された特定記憶領域を備えることで、自身が任意の電子機器に装着されて使用される場合に、当該電子機器の無効化を上記ボケーション情報に従って制御可能としたことを特徴とする。

【0010】

このように本発明の記憶媒体においては、その特定記憶領域にリボケーション情報が予め登録された構成とすることで、当該ボケーション情報で表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることが可能となる。

【0011】

ここで、記憶媒体を、メモリカードのように、記憶メディア部とコントローラとが一体化された構成とし、当該記憶媒体が任意の電子機器に装着されて使用される場合に、上記コントローラが当該電子機器から当該電子機器を表す情報を受け取って、その情報によりリボケーション情報を参照し、その参照結果に応じて当該電子機器の無効化を制御するならば、記憶媒体側で不当な電子機器によるコンテンツの記録または再生を抑止することが可能となる。

【0012】

また、上記特定記憶領域を、読み出し専用の不揮発性メモリ上に確保するか、或いは秘匿された特定手続以外ではアクセスできない書き換え可能な不揮発性メモリ上に確保するならば、リボケーション情報の改ざんにも対処可能となる。

【0013】

なお本発明は、上記構成の記憶媒体を使用したコンテンツ保護方法としても成立する。

【0014】

【発明の実施の形態】

以下、本発明の実施の形態につき図面を参照して説明する。

【0015】

図1は本発明の一実施形態に係るコンテンツ利用管理システム1の構成例を示す。なお、ここでは、コンテンツ（デジタルコンテンツ）として音楽データを一例として用いているが、この場合に限らず、映画や、ゲームソフト等のデータであってもよい。

【0016】

EMD (Electronic Music Distributor) は、音楽配信サーバまたは音楽配信放送局である。

【0017】

コンテンツ利用管理システム（以下、LCM (Licence (SDMI-)Compliant Module) と称する）1は、例えば、パーソナルコンピュータ（PC）を用いて実現される。このLCM1におけるコンテンツ保護の方法は、コンテンツを記録すべき記憶メディア（記憶媒体）13毎に、その記憶メディアの識別情報（メディアID）を用いてコンテンツの暗号化／復号化を管理することを前提としている。

【0018】

LCM1は、複数のEMD（ここでは、EMD#1～#3）に対応した受信部#1～#3を有しており、当該受信部#1～#3を通してEMDが配信する暗号化コンテンツまたはそのライセンス（利用条件と暗号化コンテンツ復号キー）などを受信する。受信部#1～#3は、再生機能や課金機能を有していても良い。また、課金機能を利用して、気に入ったコンテンツを購入することが可能である。

【0019】

LCM1は、セキュア・コンテンツ・サーバ（ここでは、Secure Music Serve

r: SMSであり、以下SMSと称する) 2を有する。このSMS 2は、利用者が購入した暗号化コンテンツをEMDI/F (インタフェース) 部3を経由して受け取る。暗号化コンテンツ (ここでは音楽コンテンツ) は、必要に応じてEMDI/F 部3で復号され、形式変換や再暗号化が施される。SMS 2は暗号化コンテンツを受け取ると、それを音楽データ格納部10に格納し、音楽データ復号鍵 (コンテンツ復号キー) をライセンス格納部9に格納する。ここでSMS 2は、配信された音楽コンテンツを利用者が試聴するために再生機能を有していても良く、この場合、SMS 2が管理する音楽コンテンツをPC上で再生することができる。

【0020】

SMS 2はまた、メディアI/F部6に装着可能なメモリカード等の記憶メディア (以下、PM (Portable Memory) と称する) 13に対してコンテンツデータ (デジタルコンテンツ) を当該I/F部6経由で出力する機能を有している。このPM 13は、図2に示す構成の専用の記録再生装置 (以下、簡単にPD (Portable Device) と称する) 12にセットして用いることで、当該PM 13に記録されたコンテンツをPD 12上で再生することができる。

【0021】

SMS 2からPM 13へのコンテンツの記録は、メディアI/F部6を通じて直接行われるか、またはPD 12を経由して行うことができる。

【0022】

ここで、LCM 1によるチェックイン/チェックアウト機能について簡単に説明する。

チェックアウトとは、LMS 1が「親」としてのコンテンツを格納しており、PM 13に、その複製を「子」コンテンツとしてコピーすることをいう。「子」コンテンツは基本的にはPD 12で自由に再生することが可能であるが、「子」から「孫」コンテンツを作成することは許されない。「親」が幾つ「子」を生むことができるかは、「親」の属性として定義される。また、チェックインとは、例えば、PM 13をLCM 1のメディアI/F部6に装着し、LCM 1が「子」コンテンツを消去 (または利用不能) することで、LCM 1内の「親」コンテン

ツは「子」を1つ作る権利を回復することをいう。これを「親」にチェックインするともいう。

【0023】

PM13は、図3に示すように、コントローラ130と、公開領域131及び秘匿領域134からなる記憶メディア部とから構成される。秘匿領域134は、コントローラ130を通して非公開の手順（つまり秘匿された特定手続）でしかアクセスできない記憶領域であり、コンテンツ復号に必要な情報を記憶するのに用いられる。秘匿領域134は、対応するPM13に固有のメディア識別情報（以下、メディアキーと称する） K_M 等の定数が記憶される秘匿ROM領域と、ライセンスする側から提供される（メディアマークと呼ばれる）秘密データであるライセンス復号キー等の変数が記憶される秘匿R/W（リード/ライト）領域からなる。メディアキー K_M は、各PM13に固有であればよく、シリアル番号や製造番号（PM13個々の製造番号、または製造ロット番号）、他の様々な識別情報を用いることができる。なお、メディアキー K_M を、各PM13に固有な識別情報とライセンス復号キーから生成するようにしても構わない。秘匿ROM領域は例えばROM（読み出し専用の不揮発性メモリ）上に確保され、秘匿R/W領域は例えばフラッシュメモリ（書き換え可能な不揮発性メモリ）の特定領域に確保される。

【0024】

公開領域131は、秘匿領域以外の、通常の手順にてアクセス可能な領域であり、読み出し専用の公開領域（以下、公開ROM領域と称する）132と、書き換え可能な公開領域（以下、公開R/W領域と称する）133からなる。公開ROM領域は例えばROM上に確保され、公開R/W領域は例えばフラッシュメモリ上に確保される。この公開ROM領域、公開R/W領域は、先の秘匿ROM領域が確保されるROM、秘匿R/W領域が確保されるフラッシュメモリ上に、それぞれ確保されるようにしても構わない。

【0025】

公開ROM領域132には、本発明に直接関係するリボケーション情報が対応するPM13の出荷段階で予め登録されている。このリボケーション情報は、コ

ンテンツの保護のためにPM13の利用を無効化すべき機器(LCM, PD)、更に具体的に述べるならばPM13(内の公開R/W領域133)を対象とするデジタルコンテンツの記録または再生のためのアクセス要求を無効化すべき機器(LCM, PD)が判別可能な情報である。本実施形態において、リボケーション情報は無効化すべき機器の識別情報(デバイスID)のリストである。そこで、以下の説明では、「リボケーション情報」に代えて「リボケーションリストRL」なる用語を用いる。つまり、公開ROM領域132には、リボケーションリストRLが予め登録されている。

【0026】

公開R/W領域133には、暗号化されたコンテンツキー(コンテンツ復号キー)、暗号化されたコンテンツ等が適宜記憶される。暗号化されたコンテンツキーは、コンテンツCを復号するための(当該コンテンツCに固有の)コンテンツキー K_C を、PM13に依存するメディアキー K_M で暗号化することで取得されるものである。また、暗号化されたコンテンツ(ここでは2重に暗号化されたコンテンツ)は、 K_C で暗号化されたコンテンツ($K_C[C]$)をPM13に依存するメディアキー K_M で暗号化する($K_M[K_C[C]]$)ことで取得されるものである。

【0027】

LCM1、PD12もまた、図4に示すようにPM13と同様の記憶領域を有している。

即ちLCM1は、公開ROM領域112及び公開R/W領域113からなる公開領域111と、非公開の手順でしかアクセスできない秘匿領域114との各記憶領域を有している。公開R/W領域113には、図1に示す音楽データ格納部10が確保されている。秘匿領域114には、LCM1の識別情報(デバイスID) ID_{LCM} が予め記憶されている。秘匿領域114にはまた、各コンテンツ毎のコンテンツキー K_C が適宜記憶される。秘匿領域114には更に、図1に示す宿帳格納部8が確保されている。SMS2の管理下にある音楽データ格納部10(公開R/W領域113)にて保持される全ての音楽コンテンツは、その識別情報であるコンテンツID(TID)と予め定められた複製可能コンテンツ数、即

ち子の残数とチェックアウトリストとをその属性情報として持つ。この属性情報を宿帳と呼び、(秘匿領域 114 内の)宿帳格納部 8 に格納される。LCM1 は、SMS2 にてこの宿帳格納部 8 にアクセスするための秘匿された特定の手续が行われた後、宿帳格納部 8 (を提供する秘匿領域 114) からデータを読み取るための秘匿領域ドライバ 7 を有している。なお、この宿帳は本発明に直接関係しないため、その利用方法の詳細については説明を省略する。

【0028】

一方、PD12 は、公開 ROM 領域 122 及び公開 R/W 領域 123 からなる公開領域 121 と、非公開の手順でしかアクセスできない秘匿領域 124 との各記憶領域を有している。秘匿領域 124 には、PD12 の識別情報 ID_{PD} が予め固定記憶されている。秘匿領域 124 にはまた、各コンテンツ毎のコンテンツキー K_C が適宜記憶される。

【0029】

図 2 は、PD12 の構成例を示す。

PM13 は、PD12 のメディア I/F 部 12f に装着して利用される。LCM1 が PD12 を介して PM13 に読み書きする場合は、LCM1 内の PDI/F 部 5、PD12 内の LCM I/F 部 12e、メディア I/F 部 12f を経由して当該 PM13 の秘匿領域 134 (図 3 参照) にアクセスする。メディア I/F 部 12f は、PM13 の秘匿領域 134 にアクセスするための秘匿領域アクセス部 (図示せず) を有している。PD12 内の公開 R/W 領域 123 及び秘匿領域 124 (図 4 参照) は、例えばフラッシュメモリ 12d 上に確保されている。また公開 ROM 領域 122 (図 4 参照) は、ROM 12c 上に確保されている。この ROM 12c には、PM13 との間で相互認証を行うためのプログラムが書き込まれている。PD12 では、CPU 12a の制御のもと、このプログラムに従って PM13 との間の相互認証等の処理が実行される。

【0030】

次に、本実施形態の動作について、EMD から配信された暗号化された音楽コンテンツを LCM1 の EMD I/F 部 3 で受信して、SMS2 により音楽データ格納部 10 に一時格納した後、その「複製」を「子」コンテンツとして、例えば

メディア I / F 部 6 に装着された PM 1 3 に記録 (コピー) するチェックアウト時の動作を例に、図 5 の流れ図を参照して説明する。

【 0 0 3 1 】

この場合、チェックアウトの指示が例えば LCM 1 のユーザインタフェース (I / F) 部 1 5 を介してなされ、且つ PM 1 3 が LCM 1 のメディア I / F 部 6 に装着された段階で、LCM 1 のメディア I / F 部 6 と PM 1 3 のコントローラ 1 3 0 との間で周知の相互認証が行われる (ステップ S 1 0 1)。この相互認証は、LCM 1 を機器 A、PM 1 3 を機器 B とすると、次のように行われるのが一般的である。

【 0 0 3 2 】

まず、機器 A から機器 B を認証するものとする。ここで機器 A は、公開鍵 k_p を保持しており、機器 B は、機器 A との間で所定のコンテンツ保護機能を共有しているならば、公開鍵 k_p に対応する秘密鍵 k_s を保持している。機器 A は乱数 R を発生して機器 B に送る。機器 B は、機器 A で発生された乱数 R を受け取ると、それを秘密鍵 k_s で暗号化して、その暗号化された乱数 ($k_s [R]$ と表す) を機器 A に返す。機器 A では、公開鍵 k_p を用いて、 $k_s [R]$ を復号し、復号結果が先に発生した乱数 R に等しければ、機器 B は正しい相手であると判定する。

【 0 0 3 3 】

その後、上記と同じことを機器 B から機器 A に対して行うことで、相互認証を行うことができる。この場合、機器 B は公開鍵を保持し、機器 A は秘密鍵を保持し、機器 A が機器 B にて発生した乱数を秘密鍵で暗号化してそれを機器 B で公開鍵を用いて復号し、先に発生した乱数に等しいかを確認する。

【 0 0 3 4 】

以上の相互認証 (S 1 0 1) により、LCM 1 及び PM 1 3 の双方にて正当な相手であることが確認されたとき、LCM 1 のメディア I / F 部 6 と PM 1 3 のコントローラ 1 3 0 との間でキー交換が行われ、同一の認証鍵 (K_{X1}) が共有される。このキー交換は、例えば DVD-ROM のコンテンツ暗号化アルゴリズムとして使用されている CSS (Content Scrambling System) に代表されるラン

ダムチャレンジ・レスポンスを用いた方法により行われる。認証鍵 (K_{X1}) は毎回代わる時変キーである。

【0035】

LCM1のメディアI/F部6は、秘匿領域114に秘匿（記憶）されている自身の識別情報 ID_{LCM} を読み出して当該 ID_{LCM} を認証鍵 (K_{X1}) で暗号化し、その暗号化された ID_{LCM} ($=K_{X1} [ID_{LCM}]$) をメディアI/F部6からPM13に送る（ステップS102）。

【0036】

PM13のコントローラ130は、LCM1側からの $K_{X1} [ID_{LCM}]$ を、先のキー交換で取得した認証鍵 (K_{X1}) で復号し、 ID_{LCM} を得る（ステップS103）。

次にPM13のコントローラ130は、復号したLCM1の識別情報 ID_{LCM} により公開ROM領域132内のリボケーションリストRLを参照し、当該 ID_{LCM} に一致する識別情報が登録されているか否かにより、LCM1によるPM13の利用を無効化するか否かを判定する（ステップS104）。

【0037】

もし、 ID_{LCM} に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するLCM1によるPM13の利用を無効化（リボケート）すべきものと判定し、以降の処理を停止する。

【0038】

これに対し、 ID_{LCM} に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するLCM1によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキー K_M を読み出し出力する（ステップS105）。そしてコントローラ130は、LCM1のメディアI/F部6との間で（当該LCM1のメディアI/F部6を介して）キー交換を行い、同一の認証鍵 (K_{X2}) を共有した上で、上記読み出したメディアキー K_M を認証鍵 (K_{X2}) で暗号化し、その暗号化された K_M ($=K_{X2} [K_M]$) をLCM1に送る（ステップS106）。

【0039】

LCM1のメディアI/F部6は、PM13側からの $K_{X2}[K_M]$ を、先のキー交換で取得した認証鍵(K_{X2})で復号し、メディアキー K_M を得る(ステップS107)。

次にLCM1のメディアI/F部6は、秘匿領域114に秘匿されているコンテンツキー K_C を取得したメディアキー K_M により暗号化し、その暗号化された $K_C (=K_M[K_C])$ をPM13の公開R/W領域133に書き込む(ステップS108)。

【0040】

このように本実施形態では、リボケーションリストRLに従って無効化(リボケート)されたならばPM13から渡されることのない(暗号化された)メディアキー K_M を、当該PM13からLCM1が受け取って、そのLCM1の秘匿領域114に秘匿されているコンテンツキー K_C を当該メディアキー K_M により暗号化して、PM13の公開R/W領域133に書き込むようにしている。このため、LCM1とPM13との間で認証鍵の交換を行い、その認証鍵を用いてコンテンツキーの暗号化/復号化を行う方法に比べて、リボケーションリストRLで指定される無効化対象LCM(PM13を利用しようとする電子機器)を確実に無効化(排除)できる。なお、LCM1の公開R/W領域113に確保された音楽データ格納部10に蓄積されている暗号化コンテンツ($K_C[C]$)をPM13に送る際に、上記取得した K_M で更に暗号化するようにしても構わない。

【0041】

次に、PM13に格納された暗号化コンテンツをPD12上で復号して再生する場合の動作について、図6の流れ図を参照して説明する。

まず、再生の指示が例えばPD12に対してなされ、且つPM13がPD12のメディアI/F部12fに装着された段階で、PD12のCPU12aとPM13のコントローラ130との間で(前記ステップS101と同様の)相互認証が行われる(ステップS201)。そして、この相互認証(S201)により、PD12及びPM13の双方にて正当な相手であることが確認されたとき、PD12のCPU12aとPM13のコントローラ130との間でキー交換が行われ、同一の認証鍵(K_{X3})が共有される。

【0042】

PD12のCPU12aは、秘匿領域124に秘匿されている自身の識別情報ID_{PD}を読み出して当該ID_{PD}を認証鍵(K_{X3})で暗号化し、その暗号化されたID_{PD}(= K_{X3} [ID_{PD}])をメディアI/F部12fからPM13に送る(ステップS202)。

【0043】

PM13のコントローラ130は、PD12側からの K_{X3} [ID_{PD}]を、先のキー交換で取得した認証鍵(K_{X3})で復号し、ID_{PD}を得る(ステップS203)。

次にPM13のコントローラ130は、復号したPD12の識別情報ID_{PD}により公開ROM領域132内のリボケーションリストRLを参照し、当該ID_{PD}に一致する識別情報が登録されているか否かにより、PD12によるPM13の利用を無効化するか否かを判定する(ステップS204)。

【0044】

もし、ID_{PD}に一致する識別情報がリボケーションリストRLに登録されている場合には、コントローラ130は該当するPD12によるPM13の利用を無効化(リボケート)すべきものと判定し、以降の処理を停止する。

【0045】

これに対し、ID_{PD}に一致する識別情報がリボケーションリストRLに登録されていない場合は、コントローラ130は該当するPD12によるPM13の利用が許可されているものと判定し、秘匿領域134に秘匿されているメディアキー K_M を読み出し出力する(ステップS205)。そしてコントローラ130は、PD12のCPU12aとの間で(当該PD12のメディアI/F部12fを介して)キー交換を行い、同一の認証鍵(K_{X4})を共有した上で、上記読み出したメディアキー K_M を認証鍵(K_{X4})で暗号化し、その暗号化された K_M (= K_{X4} [K_M])をPD12に送る(ステップS206)。

【0046】

PD12のCPU12aは、PM13側からの K_{X4} [K_M]を、先のキー交換で取得した認証鍵(K_{X4})で復号し、メディアキー K_M を得る(ステップS20

7)。

次にPD12のCPU12aは、PM13の公開R/W領域133に記憶されている暗号化されたコンテンツキー $K_C (=K_M [K_C])$ を読み込んで、ステップS207で取得したメディアキー K_M により復号し、その復号されたコンテンツキー K_C を秘匿領域124に書き込んで秘匿化する(ステップS208)。したがってPD12では、この復号されたコンテンツキー K_C (と、必要ならば先に復号化したメディアキー K_M と)を利用して、PM13の公開R/W領域133に記憶されている暗号化コンテンツを復号して再生することが可能となる。

【0047】

このように本実施形態では、リボケーションリストRLに従って無効化(リボケート)されたならばPM13から渡されることのない(暗号化された)メディアキー K_M を、当該PM13からPD12が受け取って、当該PM13の秘匿領域134に秘匿されている暗号化コンテンツキー($K_M [K_C]$)を、そのメディアキー K_M により復号化して、PD12の秘匿領域124に書き込むようにしている。このため、PD12とPM13との間で認証鍵の交換を行い、その認識鍵を用いて暗号化コンテンツキーの復号化を行うのに比べて、リボケーションリストRLで指定される無効化対象PD(PM13を利用しようとする電子機器)を確実に無効化できる。

【0048】

なお、以上の実施形態では、LCM1とPM13の間、PD12とPM13の間で、秘匿領域に秘匿されている情報、または秘匿領域に秘匿すべき情報の授受を行う際に、当該情報を認証鍵(K_{Xi})により暗号化するものとしたが、認証鍵による暗号化は必ずしも必要ではない。但し、コンテンツ保護をより確実なものとするには、認証鍵による暗号化を行うことが好ましい。

【0049】

また、以上の実施形態では、リボケーションリストRLが公開ROM領域132に登録されているものとして説明したが、リボケーションリストRLが改ざんされない領域であれば良く、例えば秘匿された特定手続でしかアクセスできない秘匿領域134に登録されるようにしても良い。

【 0 0 5 0 】

【発明の効果】

以上詳述したように本発明によれば、記憶媒体の特定記憶領域に、コンテンツ保護のために無効化すべき電子機器が判別可能なリボケーション情報が予め登録された構成としたので、当該記憶媒体が上記リストで表される電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることができる。

【図面の簡単な説明】

【図 1】

本発明の一実施形態に係るコンテンツ利用管理システムのブロック構成図。

【図 2】

図 1 中の PD（記録再生装置） 1 2 のブロック構成図。

【図 3】

図 1 中の PM（記憶メディア） 1 3 のブロック構成図。

【図 4】

LCM 1、PD 1 2 の記憶領域構成例を示す図。

【図 5】

LCM 1 から PM 1 3 へのコンテンツ記録時の動作手順を説明するための図。

【図 6】

PM 1 3 に格納された暗号化コンテンツを PD 1 2 上で復号して再生する場合の動作手順を説明するための図。

【符号の説明】

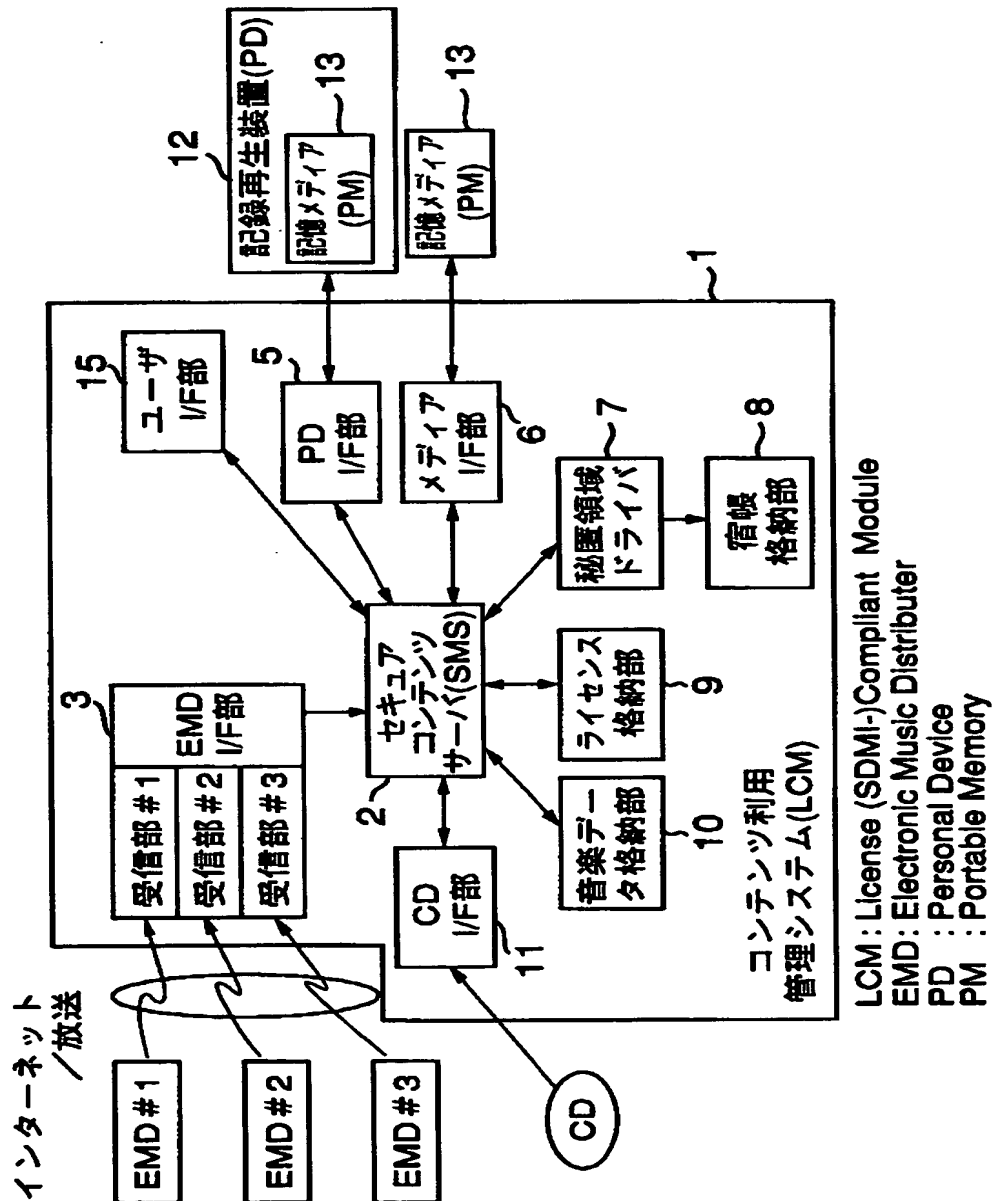
- 1 … LCM（コンテンツ利用管理システム）
- 2 … SMS（セキュア・コンテンツ・サーバ）
- 5 … PDI / F 部
- 6 … メディア I / F 部
- 7 … 秘匿領域ドライバ
- 8 … 宿帳格納部
- 9 … ライセンス格納部

- 10…音楽データ格納部
- 11…CDI/F部
- 12…PD（記録再生装置）
- 13…PM（記憶媒体、記憶メディア）
- 112, 122, 132…公開ROM領域
- 113, 123, 133…公開R/W領域
- 114, 124, 134…秘匿領域
- 130…コントローラ

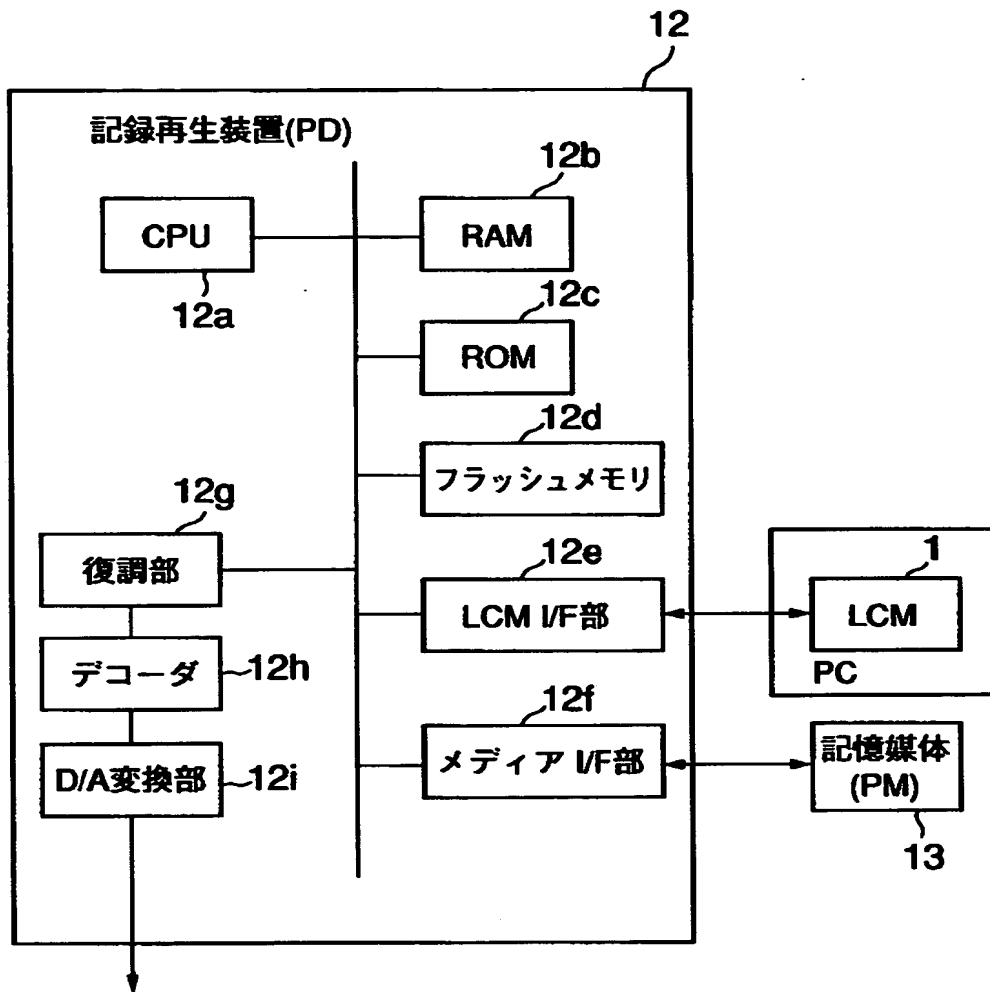
【書類名】

図面

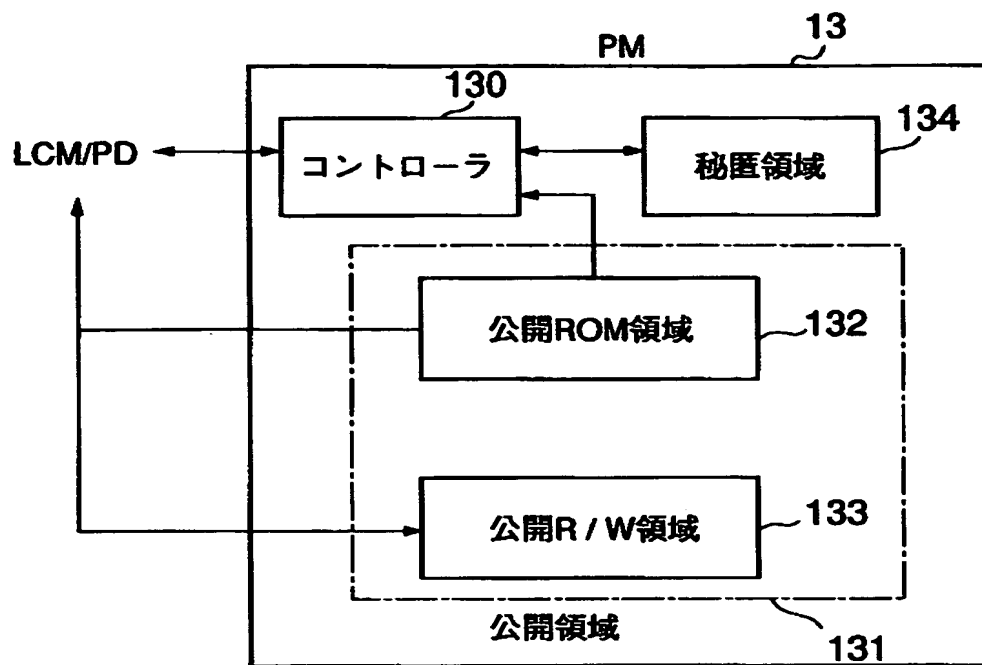
【図 1】



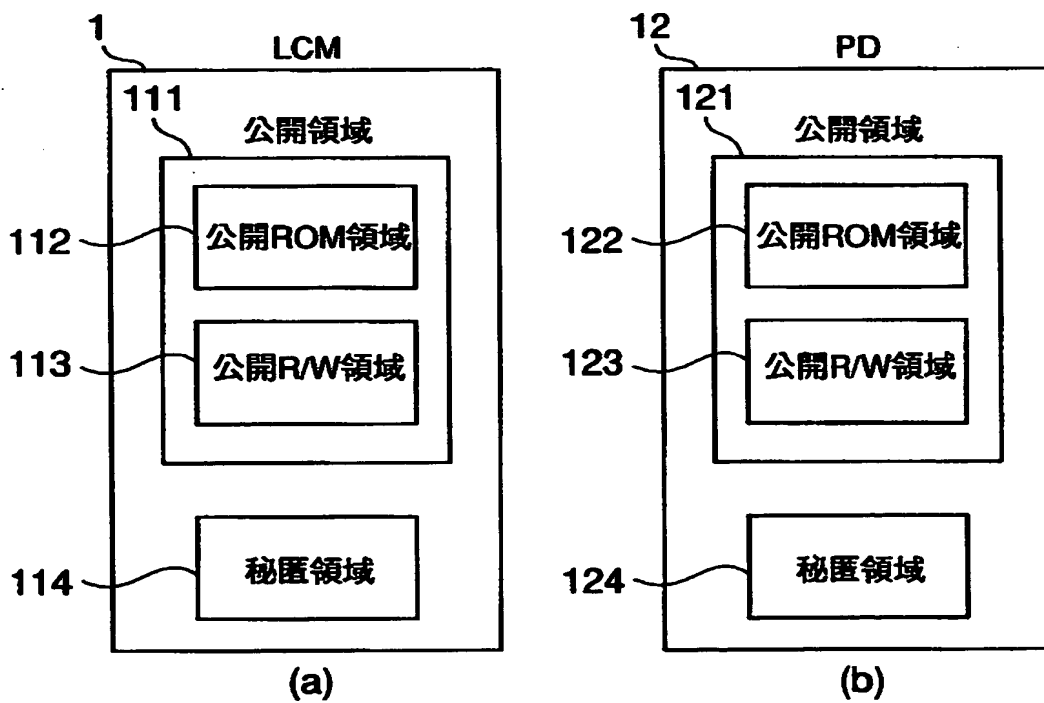
【図 2】



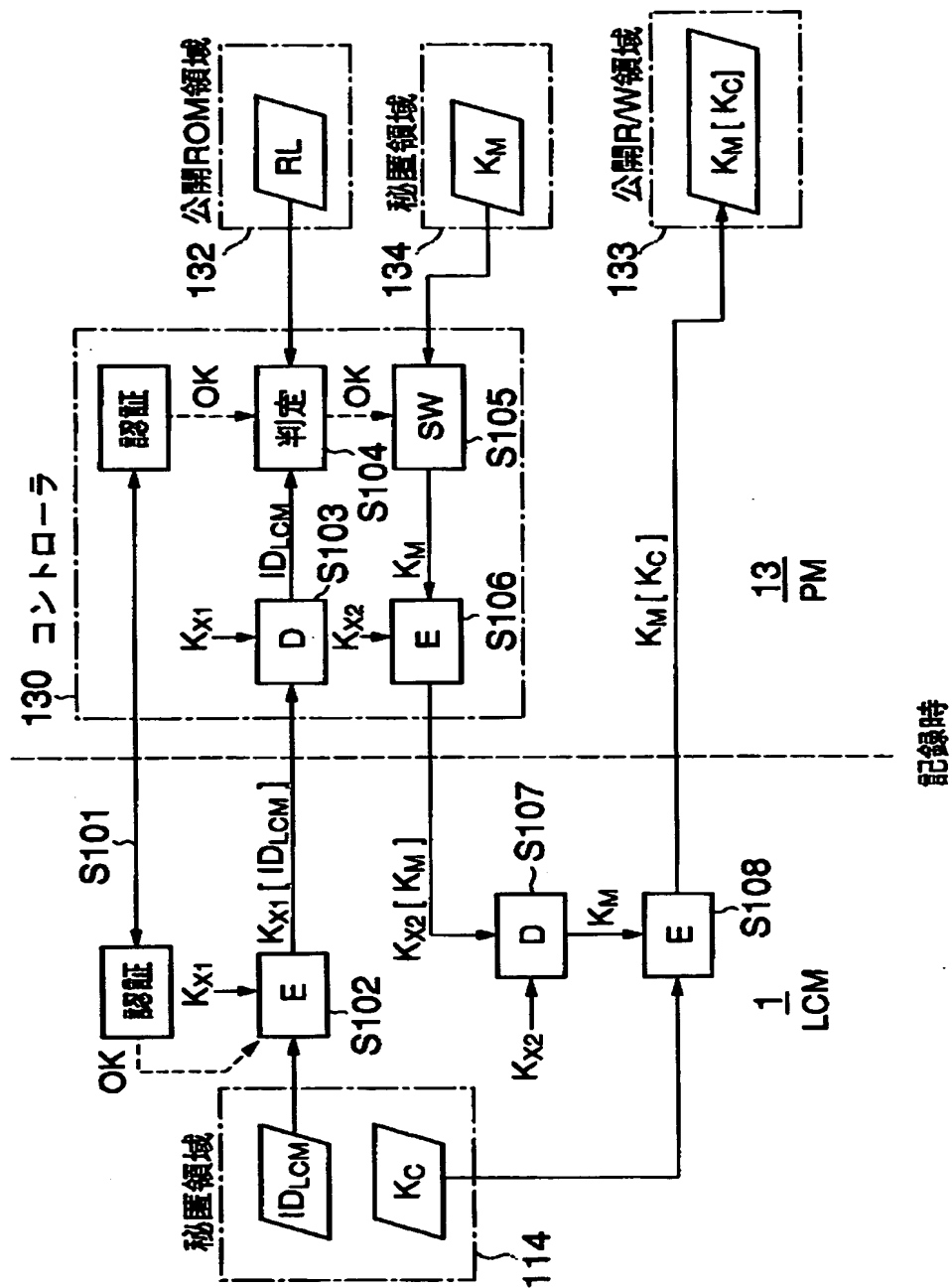
【図 3】



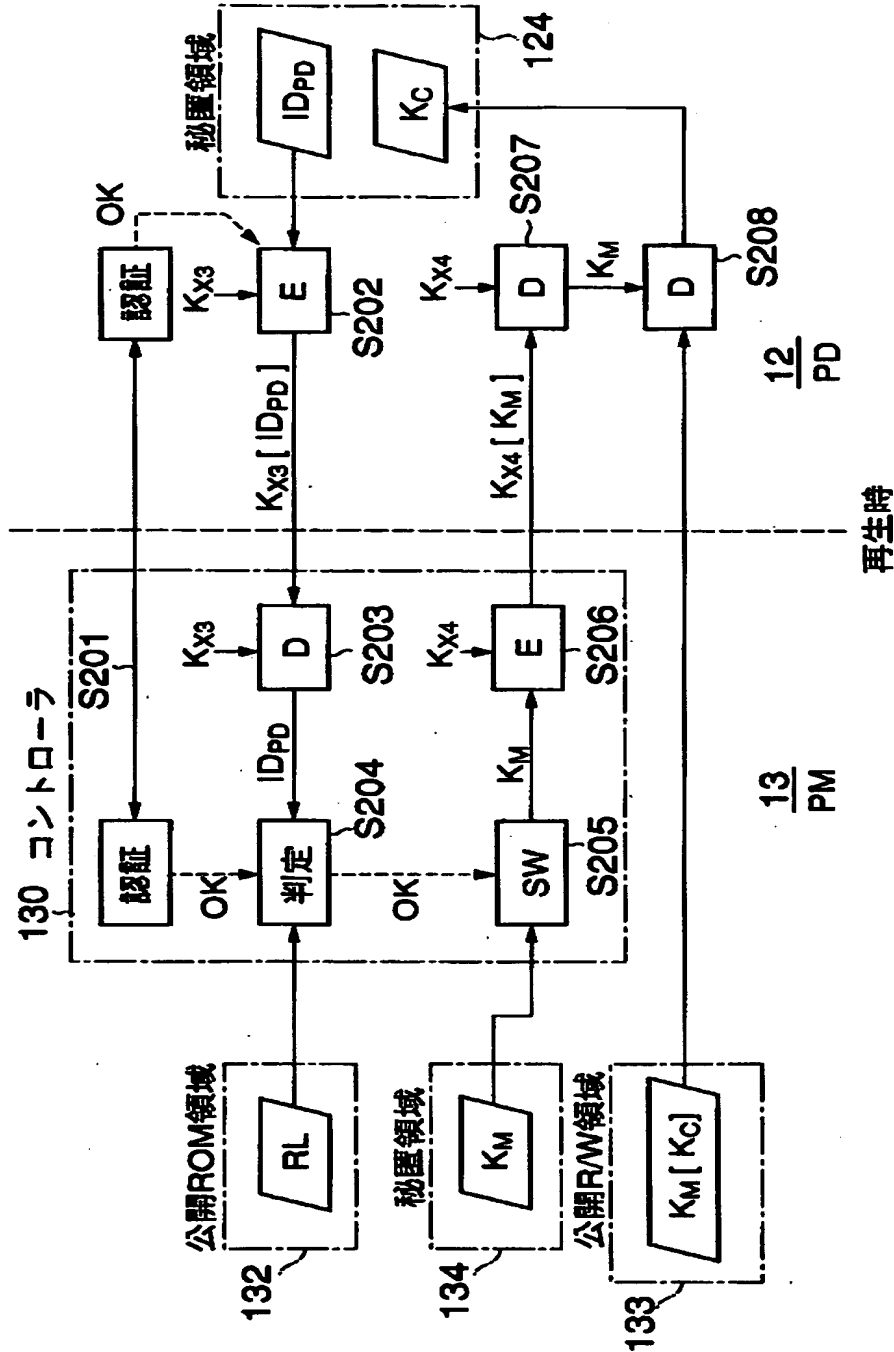
【図 4】



【図 5】



【図 6】



【書類名】 要約書

【要約】

【課題】 記憶媒体の特定記憶領域にリボケーション情報が予め登録された構成とすることで、当該記憶媒体がリボケーション情報で表される不当な電子機器に装着して使用される場合に、その電子機器を無効化してコンテンツの保護を図ることができるようにする。

【解決手段】 PM（記憶媒体）13上に確保された読み出し専用の公開ROM領域132に、コンテンツ保護のために無効化すべきPD（記録再生装置）が判別可能なリボケーションリストRLを予め登録しておき、当該PM13がLCM（コンテンツ利用管理システム）またはPDに装着して使用される場合に、PM13上に設けられたコントローラ130が、そのLCMまたはPDから、その機器を表す情報を受け取って、その情報によりリボケーションリストRLを参照し、その参照結果に応じて当該機器を無効化するか否かを決定する。

【選択図】 図3

出 願 人 履 歴 情 報

識別番号 [000003078]

1. 変更年月日	1990年 8月22日
[変更理由]	新規登録
住 所	神奈川県川崎市幸区堀川町72番地
氏 名	株式会社東芝

出 願 人 履 歴 情 報

識別番号

[000005821]

1. 変更年月日	1990年 8月28日
[変更理由]	新規登録
住 所	大阪府門真市大字門真1006番地
氏 名	松下電器産業株式会社